20. 4. 2018

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

# Privacy by design jako jedno z nových pravidel pro zpracování osobních údajů?

Obecné nařízení o ochraně osobních údajů[1], které je také známé pod svým anglickým názvem General Data Protection Regulation, resp. zkratkou GDPR, bude plně účinné od 25. května 2018. GDPR k tomuto datu jako přímo závazný evropský předpis nastaví nový právní rámec pro zpracování osobních údajů. Doprovodný český zákon, pokud jej zákonodárce do května tohoto roku vůbec přijme, upraví toliko některé dílčí aspekty.

Ve srovnání se současnou úpravou obsaženou zejména v zákoně č. 101/2000 Sb., o ochraně osobních údajů, GDPR žádnou skutečně dramatickou změnu nepředstavuje. Definice veškerých zásadních pojmů, jako je osobní údaj, citlivý osobní údaj, zpracování údajů, správce a zpracovatel, zůstává z obsahového hlediska prakticky stejná. Stejně tak GDPR přebírá základní zásady či pravidla pro zpracování osobních údajů ze současné evropské úpravy[2]. Jedná se o zásadu zákonnosti, účelového omezení, minimalizace údaje, transparentnosti zpracování atd. A do třetice i velká většina práv dotčených osob, subjektů údajů, kterou GDPR upravuje, existuje již nyní. Typicky se jedná o právo na informace o zpracování osobních údajů, právo na přístup ke kopii zpracovávaných údajů, právo na opravu, námitku, ale i o právo na výmaz.[3]

Na druhé straně GDPR některé nové instituty, které do této doby české právo oblasti zpracování osobních údajů nezná, obsahuje. Mezi nové povinnosti správce můžeme řadit zásadu doložitelné odpovědnosti, podle které správce musí nejen plnit své povinnosti dle nařízení, ale také svůj postup dokumentovat a být schopen doložit. K tomu mu GDPR nabízí, resp. ve většině případů správcům spíše ukládá, několik nových povinností. Jsou jimi zejména povinnost vést záznamy o činnostech zpracování osobních údajů, řídit případy porušení zabezpečení osobních údajů, provádět při přípravě nového zpracování osobních údajů dopadovou analýzu, tzv. posouzení vlivu na ochranu osobních údajů, některá nová zpracování konzultovat s Úřadem pro ochranu osobních údajů, jmenovat pověřence pro ochranu osobních údajů atd.[4]

Někde na pomezí pravidla pro zpracování dat a nástroje pro doložení souladu je i povinnost upravená v čl. 25. Jedná se o tzv. záměrnou ochranu osobních údajů, která je známější a snad i pochopitelnější pod anglickým názvem Data Protection by Design. Jejím obsahem je povinnost správce údajů jak v době nastavování parametrů pro nové zpracování osobních údajů, tak i v jeho průběhu, aplikovat technická a organizační opatření k zajištění toho, aby zpracování osobních údajů probíhalo v souladu s obecným nařízením a aby byla ochráněna práva dotčených osob. GDPR v tomto kontextu zmiňuje především minimalizaci zpracovávaných údajů, tedy zajištění toho, aby rozsah zpracovávaných osobních údajů byl skutečně nezbytný k dosažení účelu zpracování, resp. aby zpracování osobních údajů bylo již od počátku koncipováno v souladu s touto a dalšími zásadami pro ochranu dat.[5]

Je však skutečně tento princip v českém právu zcela nový? Domnívám se, že ani v případě záměrné ochrany dat se o revoluční předěl v českém právu ochrany zpracování osobních údajů nejedná, a to především z následujících dvou důvodů:

Již současný zákon o ochraně osobních údajů správci výslovně ukládá, aby při každém zpracování respektoval práva dotčených osob a zpracování prováděl takovým způsobem, které do těchto práv, zejména do práva na soukromí, zasáhne jen minimálním způsobem. Jedná se jak o § 10 zákona, který

tuto povinnost ukládá všem správcům a zpracovatelům bez rozdílu, a pak poněkud nekoncepčně v § 5 odst. 3, který tuto povinnost opakuje pro ta zpracování, která jsou prováděna na základě zákonného zmocnění.[6] Byť tato dvě ustanovení nehovoří výslovně o pravidlu nastavování či koncipování každého zpracování již od počátku tak, aby odpovídalo náležitostem dle relevantní právní úpravy, zásadu minimalizace zásahu do soukromí, kterou obě upravují, fakticky jinak uplatnit nelze.

Druhým aspektem či úvahou odůvodňující závěr, že princip záměrné ochrany osobních údajů tak, jak je v GDPR upraven, nepředstavuje nic dramaticky nového, vychází z toho, že nastavení prostředků či nástrojů pro zpracování dat způsobem, který odpovídá všem konkrétním požadavkům práva oblasti ochrany osobních údajů (účelové omezení, minimalizace údajů, omezená doba uchování atd.) je nedílnou součástí plnění těchto dalších pravidel jako takových. Jinak řečeno, pokud správce nesprávně nebo vůbec neaplikuje pravidlo pro omezení rozsahu shromažďovaných osobních údajů na nezbytné minimum již při nastavování pravidel celého zpracování nebo při nastavení parametrů využívaných prostředků, typicky IT systému či aplikace, obvykle bude jeho činnost s tímto pravidel v rozporu i v průběhu zpracování samotného.

Ke druhému bodu se v nedávné době poměrně ilustrativně vyslovil Městský soud v Praze. Ten se zabýval sporem Úřadu pro ochranu osobních údajů a společnosti ČSAD Karviná a.s. týkajícím se zpracovávání rodného čísla v souvislosti s vydáváním elektronického peněžního prostředku, předplacené jízdenky. Jmenovaná společnost pro vydání jízdenky vyžadovala poskytnutí osobních údajů v rozsahu jméno, příjmení, titul, rodné číslo, datum narození a trvalé bydliště. Úřad pro ochranu osobních údajů konstatoval, že rodné číslo není pro uzavření soukromoprávní smlouvy nezbytné. V činnosti účastníka řízení shledal porušení principu minimalizace, tedy v rozporu s § 5 odst. 1 písm. d) zákona o ochraně osobních údajů, za což účastníku uložil i finanční sankci. Společnost ČSAD Karviná a.s. dané rozhodnutí předsedy úřadu napadla u soudu. Argumentovala především tím, že rodné číslo je pro zpracování a evidování předplatných jízdenek nezbytné, protože příslušný software pro výdej a správu předplacených jízdenek je nastaven tak, že pro identifikaci zákazníků používá právě rodné číslo.

Městský soud v Praze však tuto argumentaci jednoznačně odmítl, když uvedl mj. následující: „Postup žalobce proto nelze aprobovat, neboť ačkoli je plnění uzavřené smlouvy, tj. poskytování přepravy cestujícím, nepochybně spjato s jeho technickou realizací, nemůže technická realizace ospravedlňovat nezákonné shromažďování osobních údajů. K uzavření smlouvy mezi cestujícím a žalobcem jednoznačně postačuje jméno, příjmení, datum narození a adresa trvalého pobytu cestujícího - žadatele o vydání EM CARD, ostatně tyto údaje jsou obecně postačující při uzavírání všech soukromoprávních kontraktů. Rodné číslo naproti tomu slouží k identifikaci občanů ve vztahu ke státu, resp. jeho orgánům. Žalobce tedy měl technicky zajistit fungování systému tak, aby elektronické odbavovací zařízení a příslušná karta či jiné technické prostředky ke svému provozu rodné číslo nevyžadovaly."[7]

Soud tak podle mého názoru potvrzuje výše naznačenou úvahu, tedy že správné nastavení rozsahu shromažďovaných údajů již od počátku a při využití veškerých nástrojů pro zpracování dat, včetně IT systémů, je nezbytnou podmínkou pro dosažení souladu s již nyní platnými předpisy pro zpracování osobních údajů. Bez správného nastavení parametrů pro zpracování osobních údajů na počátku nelze dosáhnout toho, aby zpracování jako celek bylo v souladu s příslušnými právními předpisy

**Přináší tedy GDPR v tomto bodě něco nového?**

Nerespektování zásady záměrné ochrany osobních údajů bude nově skutkovou podstatou správního deliktu dle čl. 83 odst. 4 GDPR. Za porušení této zásady může být správci uložena sankce až do výše

10 milionů EUR nebo 2 % celosvětového ročního obratu skupiny podniků za předchozí finanční rok, podle toho, která částka bude v konkrétním případě vyšší. Porušení výše uvedených ustanovení § 5 odst. 3 a § 10 zákona o ochraně osobních údajů samo o sobě deliktem nebylo.[8]

V dosavadní praxi tak tudíž nebyla řešena otázka, jaký je vztah mezi deliktem spočívajícím v porušení pravidla minimalizace zásahu do soukromí, dle GDPR záměrné ochrany osobních údajů, a deliktem spočívajícím např. ve shromažďování osobních údajů v nepřiměřeném rozsahu či jejich uchování po nepřiměřenou dobu. Tato otázka není pouhým teoretickým cvičením, protože za delikt spočívající v porušení zásady záměrné ochrany osobních údajů lze, jak je výše uvedeno, uložit sankci do výše 10 milionů EUR či 2 %  celosvětového obratu skupiny podniků, zatímco porušení pravidel minimalizace či omezení uložení spadá do kategorie deliktů, za které lze uložit pokutu až do výše 20 milionů EUR či 4 % ze světového obratu skupiny podniků.

Až praxe dozorového úřadu a případný soudní přezkum upřesní hranice mezi těmito dvěma možnými delikty. Podle mého názoru by hranice měla či mohla být hledána s ohledem na to, zda skutečně došlo k porušení některého ze základních principů pro zpracování osobních údajů, nebo zda správce pouze nedostatečně nastavil zpracování osobních údajů, ale ke skutečnému zásahu do práv dotčených osob nedošlo. Stejně tak by zjevně do skupiny deliktů s nižší hranicí sankce mohlo spadat nedostatečné nastavení a dokumentování procesu, jakým správce zásadu záměrné ochrany osobních údajů v praxi uplatňuje.

**Mgr. František Nonnemann**,
autor je zaměstnancem MONETA Money Bank, a.s.*

e-mail: nonnemann@volny.cz

_____

[*] Článek vyjadřuje osobní názor autora, nikoliv jeho zaměstnavatele.

[1] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
[2] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
[3] Ač toto právo v současném zákoně o ochraně osobních údajů ani směrnici 95/46/ES explicitně uvedeno není, podíváme-li se na výčet situací v čl. 17 odst. 1 GDPR, kdy je správce povinen osobní údaje vymazat (dosažení účelu, pro který byly údaje zpracovávány, odvolání souhlasu při neexistenci jiného právního důvodu pro zpracování, protiprávnost zpracování údajů atd.), je zjevné, že ve všech těchto situacích je povinen stejně postupovat již dnes.
[4] Srov. Nulíček, M. Donát, J. Nonnemann, F. Lichnovský, B. Tomíšek, J. GDPR/Obecné nařízení o ochraně osobních údajů. Praktický komentář. Wolters Kluwer, Praha: 2017.

[5] Princip záměrné ochrany osobních údajů tak, jak je upraven ve zmíněném ustanovení GDPR, je fakticky stručným shrnutím konceptu Privacy by Design rozvíjeného především bývalou ontarijskou komisařkou pro ochranu soukromí Ann Cavoukian. Stručný úvod do tohoto konceptu viz Cavoukian, Ann: Privacy by Design,
The 7 Foundational Principles, dostupné na na www, k dispozici >>> zde.
[6] Srov. stanovisko Úřadu pro ochranu osobních údajů č. 6/2009, Ochrana soukromí při zpracování osobních údajů, dostupné na www, k dispozici >>> zde.
[7] Rozsudek Městského soudu v Praze ze dne 7. prosince 2017 č.j. 11 A 152/2015 – 36, dostupné na www, k dispozici >>> zde.
[8] Srov. Kučerová, A. Nováková, L. Foldová, V. Nonnemann, F. Pospíšil, D. Zákon o ochraně osobních údajů. Komentář. Praha: C. H. Beck, 2012.



## Další články:


- Nový zákon o veřejných dražbách, aukce a obálkové metody
- Pohled přes hranice – natáčení pornografických klipů jako důvod výpovědi z nájmu bytu
- Nařízení EU o umělé inteligenci a jeho dopady na využití jazykových modelů v advokátní praxi
- Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi
- Kupní smlouva o převodu nemovitosti bez uvedení výše kupní ceny
- Druhá „tlačítková novela": povinné tlačítko pro odstoupení od smlouvy
- Souhlas s veřejným užíváním pozemku jako překážka nároku na bezdůvodné obohacení – nález Ústavního soudu sp. zn. I. ÚS 2541/25
- Kupní smlouva bez přesného určení kupní ceny
- Byznys a paragrafy, díl 36.: Doložka o mlčenlivosti
- Detekce podezřelého obchodu v kontextu hazardních her
- AI omnibus